

1 Stephen R. Cochell
Admitted Pro Hac Vice
2 *srcochell@gmail.com*
5850 San Felipe, Ste. 500
3 Houston Texas 77057
Telephone: (713) 436-8000
4 Facsimile: (213) 623-2000

5 Allan Grant (SBN#213658)
Grant's Law Firm
6 17351 Greentree Drive
Riverside, California 92503-6762
7 Telephone (888)937-7555
Facsimile (866)858-6637

8 Attorneys for Defendant
9 JASON EDWARD THOMAS CARDIFF

10
11 UNITED STATES DISTRICT COURT
12 CENTRAL DISTRICT OF CALIFORNIA

13 UNITED STATES OF AMERICA,

Case No. 5:23-CR-00021-JGB

14 Plaintiff,

15 vs.

16 JASON EDWARD THOMAS
CARDIFF,

17 Defendant.
18

19
20 **DEFENDANT'S REPLY MEMORANDUM IN SUPPORT OF MOTION TO**
21 **DISMISS COUNT TWO OF THE INDICTMENT**
22
23
24
25
26
27
28

TABLE OF CONTENTS

TABLE OF CONTENTS	ii
TABLE OF AUTHORITIES.....	iii
DEFENDANT'S REPLY MEMORANDUM IN SUPPORT OF MOTION TO DISMISS COUNT TWO OF THE INDICTMENT	1
I. The <i>Dubin</i> Analysis Revisited	1
II. The Government's Argument	4
III. The Government's Other Authorities Show That <i>Dubin Controls</i> Applies this Case.	7
IV. Conclusion.....	10

TABLE OF AUTHORITIES

Case Law

Dubin v. United States, 599 U.S. 110 (2023) *passim*

United States v. Felch, 2024 U.S. Dist. LEXIS 16474 (D.N.M. Jan. 22, 2024) 6-10

United States v. Iannelli, 700 F. Supp.3d 1 (D. Mass. 2023) 8-10

United States v. Ovsepian, 113 F.4th 1193 (9th Cir. 2024) 1-4, 10

Statutes

18 U.S.C.S. § 1028A Aggravated Identify Theft *passim*

1 **DEFENDANT'S REPLY MEMORANDUM IN SUPPORT OF MOTION TO**
2 **DISMISS COUNT TWO OF THE INDICTMENT**

3 The Government's arguments fail to acknowledge the key principles in both
4 *United States v. Dubin*, 599 U.S. 110 (2023) and *United States v. Ovsepian*, 113 F.4th
5 1193 (9th Cir. 2024), which clarify that incidental use of identity information for
6 billing purposes does not amount to aggravated identity theft.

7 The Government's reliance on pre-Dubin cases and focus on "how" credit cards
8 were processed fails to take this case outside the scope of the Supreme Court's test in
9 *Dubin*. *Dubin* teaches that courts must focus on the "who" in determining whether
10 the means of identification was at the crux of the fraud or ancillary to any alleged
11 criminality. Redwood did not use credit card information to impersonate its customers
12 or to deceive anyone into believing that a different person was initiating the charges.
13 Instead, the charges were made using the legitimate identities of real customers who
14 had already provided their information voluntarily in prior transactions. This lack of
15 deception about *who* was being charged is critical because, as the Court emphasized
16 in *Dubin*, the statute does not reach situations where a legitimate identity is used
17 without consent to process additional charges.

18 The Court expressly held that Congress did not intend for §1028A to transform
19 every billing dispute or overbilling scheme involving the use of a name, number, or
20 other means of identification into an aggravated identity theft offense. Thus, because
21 there was no misrepresentation that changed *who* was involved, but rather only a
22 dispute about *how* the information was used, the use of identity information in this
23 case is insufficient to constitute aggravated identity theft under the *Dubin* standard.

24 **I. The *Dubin* Analysis Revisited**

25 In *Dubin*, the Supreme Court held that the words "use" and "in relation to" in 18
26 U.S.C. §1028A should not be read so broadly that the statute would "apply
27 automatically any time a name or other means of identification happens to be part of
28 the payment or billing method used in the commission of a long list of predicate

1 offenses." *Dubin*, 599 U.S. at 1564-65 (emphasis supplied). Instead of addressing the
2 "who" in the transactions, the Government in this case argues "how" transactions were
3 processed and attempts to support its positions with Ninth Circuit decisions that pre-
4 date *Dubin* or cases that simply do not stand for the Government's arguments. Dkt.
5 111 at 13-19. This argument was rejected in *Dubin* and should be rejected in this
6 case.

7 A "defendant 'uses' another person's means of identification 'in relation to' a
8 predicate offense when this use is at the crux of what makes the conduct
9 criminal." *Dubin*, 599 U.S. at 1573. Section 1028A's reach is thus limited to
10 situations where "a genuine nexus" exists between the use of a means of identification
11 and the predicate offense. *Id.* at 1565. However, § 1028A still proscribes use of a
12 means of identification involving fraud or deceit about identity. *Id.* at 1570. The
13 statute focuses on "offenses built around what the defendant does with the means of
14 identification in particular. *Id.* at 1568. "In other words, the means of identification
15 specifically [must be] a key mover in the criminality." *Id.*

16 With respect to the conduct at issue in *Dubin*, the Court reasoned that the
17 defendant's "use of the patient's name was not at the crux of what made the underlying
18 overbilling fraudulent." *Id.* "The crux of the healthcare fraud was a misrepresentation
19 about the qualifications of [the defendant's] employee," and so, "[t]he patient's name
20 was an ancillary feature of the billing method employed." *Id.* In all, the Court
21 explained that the "fraud was in misrepresenting *how* and *when* services were
22 provided to a patient, not *who* received the services," and for that reason, the
23 defendant's conduct did not provide a basis for prosecution under §
24 1028A(a)(1). *Id.* (emphasis in original).

25 Just as in *Dubin*, Cardiff did not misrepresent the customer's identity. As in
26 *Dubin*, where the use of each Medicaid numbers was incidental, the processing of
27 transactions through encrypted credit card data was ancillary to the alleged fraudulent
28 nature of the predicate offense. The crux of the alleged fraud in this case is whether a

1 customer was overcharged by placing customers on continuity without authorization.

2 This case falls within the examples provided by the *Dubin* court. The Court, in *Dubin*,
3 rejected a broad interpretation of § 1028A(a)(1) that would encompass any incidental
4 use of identification in the commission of a predicate offense. This Court should
5 similarly reject the Government's attempt to avoid the holding in *Dubin*.

6 As in *Dubin*, the question is whether Cardiff committed aggravated identity
7 theft triggering a mandatory 2-year prison sentence. The Court rejected the notion
8 that the statute applied as long as a billing or payment method employs another
9 person's name or other identifying information.

10 On that sweeping reading, as long as a billing or payment
11 method employs another person's name or other
12 identifying information, that is enough. A lawyer who
13 rounds up her hours from 2.9 to 3 and bills her client
14 electronically has committed aggravated identity theft.
15 The same is true of a waiter who serves flank steak but
charges for filet mignon using an electronic payment
method.

16 The text and context of the statute do not support such a
17 boundless interpretation. Instead, §1028A(a)(1) is
18 violated when the defendant's misuse of another
19 person's means of identification is at the crux of what
20 makes the underlying offense criminal, rather than
21 merely an ancillary feature of a billing method. Here,
22 the crux of petitioner's overbilling was inflating the
value of services actually provided, while the patient's
means of identification was an ancillary part of the
Medicaid billing process.

23 *Dubin*, 599 U.S. at 1563 (emphasis supplied).
24

25 Similarly, in *Ovsepien*, the Government argued that Ovsepien's possession of
26 a patient file and maintenance of the file facilitated the crime. Court's analysis
27 provides further insight into this case:

28 Although *Dubin* undoubtedly "used" a patient's means of

1 identification in the literal sense when he submitted the
2 fraudulent billing containing the patient's name and
3 Medicaid reimbursement number, the "use of the
4 patient's [information] was not at the crux of what made
5 the underlying overbilling fraudulent." *Id.* Rather, "[t]he
6 crux of the healthcare fraud" in Dubin's case "was a
7 misrepresentation about the qualifications of [Dubin's]
8 employee." *Id.* Dubin "misrepresent[ed] how and when
9 services were provided to a patient," but he did not
10 misrepresent "who received the services." *Id.* His "use"
11 of the patient's identifying information, therefore, did not
12 fall within the meaning of § 1028A(a)(1). *Id.* Although
13 *Dubin* concerned only the "use" prong of § 1028A(a)(1),
14 the Court explained that for each of the verbs "the means
15 of identification [must] be at the crux of the criminality"
16 of the charged predicate offense. *Id.* at 127; *see id.* at 132.

17 *Ovsepien*, 113 F.4th at *24. Both *Dubin* and *Ovsepien* held that merely facilitating a
18 predicate offense is insufficient under 1028A, because the means of identification
19 must be integral to what made the conduct fraudulent. *Id.* at *28. In both cases, the
20 use of identity information (credit card numbers in this case, a patient file in *Ovsepien*)
21 was not used to deceive anyone about "who" was involved in the transaction. In
22 Cardiff's case, the fraud (if any) concerns how the transactions were processed, not
23 the misuse of the customers' identities. Just as the Ninth Circuit found that the
24 possession of the patient file was insufficient to trigger aggravated identity theft
25 charges in *Ovsepien*, the use of encrypted customer credit card data for billing does
26 not meet the heightened standard of identity theft under § 1028A in this case.

27 **II. The Government's Argument**

28 The Government cherry-picks different portions of the Dubin decision to try to
suggest that internal procedures (the "how") to charge a customer's pre-existing
account somehow transform encrypted credit card numbers into aggravated identity
theft under § 1028A. The Government asserts that identity theft covers both situations
when someone steals personal information about and belonging to another...and uses

1 the information to deceive others. Dkt. 111 at 8. The Government further states that
2 identity theft thus intermingles aspects of theft and fraud, misappropriation and
3 deceitful use, concluding that the three verbs in § 1028A capture this complexity and
4 the terms “uses” supplies the crux of deceit in this case. However, this argument
5 stands in stark contrast to the Supreme Court’s holding that the focus with aggravated
6 identity theft is on the “who” and not the “how.” The Government has described the
7 *methods* of how the predicate crime of access device fraud was allegedly committed,
8 but has not established a crime of aggravated identity theft.¹

9 The Government’s “use” argument also fails to recognize that using existing
10 customer credit card information to create unauthorized charges does not *ipso facto*
11 make the use of identity central to the fraudulent scheme. *Dubin*, at 128. The *Dubin*
12 Court made it clear that: “Patient names or other identifiers [credit cards] will, of
13 course, be involved in the great majority of healthcare billing... Under the
14 Government’s own reading, such cases are ‘automatically identity theft,’...,
15 independent of whether the name itself had anything to do with the fraudulent aspect
16 of the offense.”

17
18 The charges pertained to customers who had already made legitimate purchases
19 from Redwood and received their products. Dkt. 106-2, Cardiff Dec. ¶ 9. It is
20 important to note that Redwood’s billing system did not need to use the first and last
21 names of customers to process continuity orders. Dkt. 106-2, Declaration of Jason
22 Cardiff, ¶ 9. The alleged fraudulent acts arose from unauthorized billing practices--

23 ¹ The Government also refers to a Venn Diagram that would supposedly depict two
24 heavily overlapping circles containing customer credit and debit account information.
25 Dkt 111 at 13. While this hypothetical assertion may be interesting, it is irrelevant
26 because the Supreme Court did not analyze *Dubin* using a Venn diagram. The Court
27 instructed that the “who” of a transaction must be the focus of analysis in determining
28 issues under *Dubin*.

1 not from a manipulation of identities. Redwood did not create any new identities or
2 falsify the identity of these customers. Redwood did not use the customer credit card
3 or billing information outside the customer's original intended use. The use of
4 customer information was merely a continuation of an existing relationship. This
5 established customer relationship further distinguishes this case from aggravated
6 identity theft scenarios, where the identity itself is misused to deceive others into
7 believing a false identity is involved. *See United States v. Felch*, 2024 U.S. Dist.
8 LEXIS 16474 (D.N.M. Jan. 22, 2024).

9 The Government is attempting to turn a billing dispute—unauthorized creation
10 of continuity orders—into an aggravated identity theft charge solely because customer
11 information was used in the billing system. This was precisely the type of overreach
12 the *Dubin* decision sought to prevent. The continuity orders involved legitimate
13 customer information allegedly used without customer consent, but this does not
14 equate to aggravated identity theft under § 1028A(a)(1). The government is
15 mischaracterizing Redwood's unauthorized creation of continuity orders as
16 aggravated identity theft solely because customer information was used in the billing
17 process. Under *Dubin*, the use of identity information must deceive others
18 about *who* is involved, not merely *how* a transaction is conducted. Here, the
19 fraudulent conduct was a billing dispute using legitimate customer identities without
20 consent, making it an overbilling issue rather than identity theft.

21 The Government misinterprets the significance of a spreadsheet used internally
22 *to process charges to existing customers for the same products for the same customer*,
23 a procedure identified by Limelight's Joanny Spina.² Whenever a customer is
24

25 _____
26 ² The Government alleges that Redwood processed unauthorized continuity charges
27 for 1,500 customers who had purchased a one-time product. Dkt. 111 at 3. Even if
28 this number were accurate—which the defense does not concede—it represents only
approximately 0.20% of the company's 765,000 transactions. Under *Dubin* the

1 converted from a single purchase to a continuity purchase, the Government assets that
2 would be a “new order” with their “card on file.”

3 The Government points out that card owners did not place orders for new
4 subscription plans, place new orders or authorize additional charges by going on
5 continuity. The Government then states: “In creating ‘new order on file’ transactions,
6 Defendant was **able to use** the full card account number...for the ‘purchase’ of new
7 products.” Dkt. 111 at 15 (emphasis supplied). The Government thus concedes that
8 the encrypted credit cards merely facilitated commission of the alleged predicate
9 offense and was ancillary to the deceit or deception to the customer.

10 The suggestion that any customer placed on continuity was charged for “new”
11 products is wholly unfounded and a blatant misrepresentation to this Court.
12 Moreover, this misrepresentation is illogical because the crux of the offense charged
13 in this case alleged that customers who made single purchases were placed on
14 continuity without their consent. In short, continuity means monthly charges for the
15 same products.

16 Regardless, a spreadsheet identifying “new order card on file,” merely
17 facilitated the same order for the same customer on the same credit card. The
18 Government’s attempt to spin the facts about “how” the customer was charged is
19 without merit.

20 **III. The Government’s Other Authorities Show That Dubin Controls**
21 **Applies this Case.**

22 The Government’s reliance on *United States v. Felch*, 2024 U.S. Dist. LEXIS
23 16474 (D.N.M. Jan. 22, 2024) is misplaced. *Felch* involved a case where a book
24
25 quantity of overcharges is irrelevant. What matters is whether there was any
26 misrepresentation of identity in the transaction.

1 keeper forged her employer's signature on a check made out to pay her credit card
2 company. The Court held that Felch's fraudulent use of her employer's signature
3 satisfied "who" authorized withdrawal of the funds, which was at the crux of the
4 alleged bank fraud. From that fact scenario, the Government erroneously concludes
5 that any deception as to who authorized funds falls within § 1028A. Dkt. 111 at 17-
6 18. The facts in *Felch* do not remotely resemble the facts in *Dubin* or this case. The
7 key distinction between Felch and this case is that Felch impersonated her employer
8 when she forged the signature to pay her personal credit card.

9 In *Felch*, the forged signature altered who appeared to authorize the
10 transaction, making the identity deception central to the crime. In this case, there
11 was no falsification of identities—the identities were correctly linked to legitimate
12 customers. The issue was a misuse of billing information, not a misrepresentation
13 of *who* was authorizing the charges. Therefore, under *Dubin*, Redwood's actions do
14 not meet the threshold for aggravated identity theft. Indeed, *Felch* falls under classic
15 identity theft because it involved a direct misrepresentation about *who* was behind the
16 transaction, while Redwood's case did not.

17 Similarly, *United States v. Iannelli*, 700 F. Supp.3d 1 (D. Mass. 2023), is
18 fundamentally different and does not support the Government's case. In *Iannelli*, the
19 defendant falsified the employer's consent on 43 phony vendor invoices and went into
20 the employers' accounting system to cover up the fraud. Iannelli stole the identity of
21 the parent corporation to deceive the bank that the parent corporation authorized the
22 extra check. In contrast, Redwood obtained consent to charge customer's accounts
23 for real products whereas Iannelli never had consent to pay phony invoices or false
24 invoices.

25 In addition, Iannelli was authorized to use her employer's signature stamp for
26 issuing authorized checks (e.g., to vendors or for regular expenses), but she used the
27 stamp to create checks for herself that were unauthorized and concealed the checks as
28

1 legitimate transactions. Iannelli issued herself checks worth over \$150,000 using the
2 signature stamp and falsely recorded these transactions in the employer's accounting
3 system to make them appear as employer's parent company's payments to furniture
4 vendors.

5 Iannelli's fraudulent use of the signature stamp misrepresented *who* had
6 authorized the checks. By using the signature stamp without permission, Iannelli
7 made it appear as if her employer's parent company had approved these checks, when,
8 in reality, she had no such authority. This misrepresentation was central to identity
9 theft under 18 U.S.C. § 1028A(a)(1) because it **deceived the bank** into believing the
10 employer's identity was behind the transaction. As the court noted, "[B]y whom the
11 signature on a check is authorized determines who is liable for the face amount of the
12 check." Therefore, the unauthorized use of the *employer's identity* was at the crux of
13 the fraud.

14
15 Iannelli also inflated her compensation by submitting fraudulent invoices with
16 incorrect hours worked and issued herself checks reflecting these inflated amounts.
17 Iannelli then used the signature stamp to create and cash checks for amounts she was
18 not entitled to, thereby overcharging her employer by approximately \$30,000.
19 Iannelli again used her employer's signature stamp to issue herself checks that
20 appeared to be legitimate, misrepresenting *who* was approving the payment. This
21 scenario was distinct from the second set of checks because it involved falsifying the
22 details of her own compensation, rather than issuing extra checks under the guise of
23 regular payments. However, the use of the signature stamp again falsely indicated that
24 the parent company had authorized these payments, thereby misusing the employer's
25 identity to deceive the bank.

26 Redwood did not create any misrepresentation about *who* was authorizing or
27 making the payments. The fraudulent conduct involved using legitimate customer
28 identities (existing customers) to create unauthorized continuity orders. There was no

1 false signature, false identity, or attempt to mislead others into believing a different
2 entity or person was behind the transactions. The issue was whether the customers
3 consented to the recurring charges, not whether their identities were misused to
4 mislead others. Stated differently, the fundamental difference is that in *Iannelli*,
5 the identity of the person authorizing the transactions was falsified (through the
6 unauthorized use of the signature stamp), making it aggravated identity theft. In
7 Redwood, the identities were correct, but the use of the information was without
8 consent, making it a billing fraud rather than identity theft.

9 The Government relies on pre-*Dubin* cases to support its assertion that *Dubin*
10 does not require impersonation where a defendant assumes an individual's identity
11 or attempts to pass themselves off as another. Dkt. 111 at 10.

12 **IV. Conclusion**

13 *Dubin* narrows the scope of § 1028 to avoid government overreaching and
14 charging garden variety overbilling cases. The Government's reliance on *Felch* and
15 *Iannelli* at best, reflects confusion in how *Dubin* must be applied or, at best, an attempt
16 to re-cast the facts to obtain a result favorable to the Government.

17 For the reasons set forth above, and in light of the Supreme Court's ruling in
18 *Dubin* and the Ninth Circuit's decision in *Ovsepian*, the defendant respectfully
19 requests that this Court grant the motion to dismiss Count Two of the indictment. The
20 government has failed to demonstrate that Mr. Cardiff's actions meet the criteria for
21 Aggravated Identity Theft under 18 U.S.C. § 1028A(a)(1), as the alleged conduct does
22 not involve a misrepresentation of "who" was involved in the transactions. Instead,
23 the issue at hand is related to alleged overbilling, which falls outside the scope of
24 identity theft as defined in *Dubin* and *Ovsepian*.

25
26 Respectfully submitted,

27 /s/ Stephen R. Cochell

28 Stephen R. Cochell

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SBN: 24044255
The Cochell Law Firm, P.C.
5850 San Felipe, Ste 500
Houston, Texas 77057
(346) 800-3500 – Telephone
srcochell@gmail.com

SERVICE LIST

I HEREBY DECLARE THAT THE FOLLOWING COUNSEL HAVE BEEN SERVED WITH THIS DEFENDANT'S REPLY MEMORANDUM IN SUPPORT OF MOTION TO DISMISS COUNT TWO OF THE INDICTMENT THROUGH THE COURT'S ECF OR NEXT GEN ELECTRONIC FILING SYSTEM:

E. Martin Estrada
United States Attorney
Mack E. Jenkins
Assistant United States Attorney Chief, Criminal Division
Ranee A. Katzenstein
Assistant United States Attorney Chief, Criminal Division
Valerie Makarewicz
Assistant United States Attorney Major Frauds Section
1100 United States Courthouse
312 North Spring Street
Los Angeles, CA 90012
Telephone: (213) 894-0756 Facsimile: (213) 894-6269
E-mail: Valerie.Makarewicz@usdoj.gov

Amanda Liskamm
Director, Consumer Protection Branch
Manu J. Sebastian
Brianna M. Gardner
Trial Attorneys
Consumer Protection Branch
U.S. Department of Justice
450 Fifth Street NW, Suite 6400 Washington, DC 20001
Telephone: (202) 514-0515 Facsimile: (202) 514-8742
E-mail: Manu.J.Sebastian@usdoj.gov
Brianna.M.Gardner@usdoj.gov

/S/ Stephen R. Cochell
Stephen R. Cochell